



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

Metodología de pruebas para estrategias de continuidad del negocio y recuperación de desastres

PROCESO
Gestión Estratégica de
Tecnologías de la Información
Versión 1
22/12/2022

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	METODOLOGÍA DE PRUEBAS PARA ESTRATEGÍAS DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 22/12/2022	Código: DS-E-GET-23

TABLA DE CONTENIDO

1. Introducción	3
2. Objetivos de la prueba	3
3. Marco teórico	3
4. Alcance de la Metodología de pruebas	6
4.1. Tipos de prueba	6
4.1.1. Prueba de Escritorio.....	6
4.1.2. Prueba por componentes.....	7
4.1.3 Prueba Integrada.....	7
5. Tipos de Alcance	7
6. Procedimiento de recopilación de pruebas.....	7

Sistema Integrado de Gestión

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	METODOLOGÍA DE PRUEBAS PARA ESTRATEGÍAS DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 22/12/2022	Código: DS-E-GET-23

1. Introducción

Se propone una metodología para probar la efectividad del DRP como estrategia de mitigación de riesgos de continuidad del negocio. Las pruebas le dan a la Entidad la oportunidad de identificar y prevenir problemas y fallas en los diferentes planes (Contingencias, recuperación ante desastres, contingencias asociadas y manejo de emergencias) de manera que puedan ser atendidas, preparando al MINAMBIENTE, para la materialización de un evento disruptivo por falla total de la infraestructura y servicios de TI.

2. Objetivos de la prueba


Realizar las pruebas del plan de continuidad tiene los siguientes objetivos:

- Validar el plan de continuidad.
- Practicar los procedimientos ante un incidente o desastre.
- Incrementar la conciencia y el conocimiento en el plan de continuidad.
- Actualizar y corregir el plan para que contemple los cambios en el ambiente del negocio
- Validar la efectividad de la estrategia de respecto de la mitigación del riesgo de continuidad


3. Marco teórico

La realización de las pruebas son el pilar fundamental para garantizar la actualización y el mantenimiento del plan de continuidad del negocio, en las pruebas se deben tener en cuenta los siguientes aspectos:

- Utilizar un formato para el planeamiento de las pruebas a realizar
- Garantizar la adecuada capacitación del personal en el entendimiento de la documentación del Plan de Continuidad y los documentos que están relacionados con el tipo de prueba

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	METODOLOGÍA DE PRUEBAS PARA ESTRATEGÍAS DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 22/12/2022	Código: DS-E-GET-23

- Se debe documentar los procedimientos que se seguirá dependiendo del tipo de prueba los cuales deben contener:
 - El detalle inicial del tipo de prueba que se desea realizar
 - El objetivo que se busca con el desarrollo de la prueba
 - Los procedimientos de recuperación que serán probados. Esto último implica establecer cuáles de los procedimientos descritos en el plan, serán considerados para realizar la prueba
 - El responsable de la prueba. Definir quién será responsable de la adecuada realización de la prueba y de obtener al final las conclusiones y los resultados de la misma. Esta responsabilidad puede recaer en el líder de continuidad del negocio, en el líder de infraestructura o líder de aplicaciones, en el líder o responsables de los procesos críticos a restaurar o en el líder del DRP, dependiendo del tipo y alcance de la prueba a realizar.
 - Planeación de la prueba, indicando el día, hora de inicio y la ventana de tiempo requerida para la prueba
 - Métricas de evaluación de los resultados, las cuales deben variar dependiendo del tipo de prueba que se vaya a realizar; estas, deben ser definidas por el líder de continuidad del negocio estableciendo, además, de qué forma se concluirá si los resultados de la prueba fueron o no adecuadas
 - Conclusiones de las pruebas, las pruebas deben obtener conclusiones a cerca de:
 - La información que debiera ser corregida en el Plan de Continuidad y en la valoración de los riesgos de continuidad, por deficiencias o errores encontrados durante la prueba.
 - La información que debiera ampliarse para mejorar su claridad en el plan al momento de ser utilizada
 - La información sobre elementos de riesgo que fueron identificados durante la prueba, como puede ser personal no encontrado, documentación no identificada, etc.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	METODOLOGÍA DE PRUEBAS PARA ESTRATEGÍAS DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 22/12/2022	Código: DS-E-GET-23

- Las conclusiones sobre si la documentación de los procedimientos definidos es práctica o si bien los procedimientos pueden ser mejorados para obtener mejores resultados considerando variables como tiempo, costo y esfuerzo.
- La documentación y revisión de todos los resultados generados durante la prueba es trascendental para el proceso de mejora continua
- Las pruebas del plan se deben realizar al menos una vez al año.

El Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de los Estados Unidos, en la guía de planificación de contingencia para los Sistemas de Información Federales, hace referencia al plan de pruebas y ejercicios donde establece que las pruebas son las herramientas de evaluación que utilizan métricas cuantificables para validar la operatividad de un sistema de información o componentes del sistema en un entorno operativo. Por ejemplo, una organización podría poner a prueba la lista del árbol de llamadas para determinar si las llamadas se pueden ejecutar dentro de los plazos establecidos. Una prueba se lleva a cabo lo más cercano posible a un entorno operativo y si es posible una prueba real de los componentes o sistemas utilizados en las operaciones diarias de la organización. Respecto de los ejercicios representan una simulación de una situación de emergencia diseñada para validar la viabilidad de uno o más aspectos del plan de continuidad y/o DRP. En un ejercicio el personal con funciones y responsabilidades valida el contenido de un plan a través de la discusión de sus funciones y sus respuestas a las situaciones de emergencia, la ejecución de las respuestas en un entorno operativo simulado, u otros medios de validación de las respuestas que no involucran el uso del entorno de operación real.

Se establecen ejercicios de simulación, que son ejercicios prácticos basados en la discusión donde el personal se reúne en un salón de clases o en grupos de trabajo para discutir sus roles durante una emergencia y sus respuestas a una situación de contingencia en particular. Un facilitador presenta un escenario de riesgo y les pide a los participantes preguntas relacionadas con el escenario planteado, teniendo en cuenta los roles y responsabilidades de los participantes para la toma de decisiones. Un ejercicio de simulación como este, es sólo basado en el debate y no implica el despliegue de equipos u otros recursos para su análisis.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	METODOLOGÍA DE PRUEBAS PARA ESTRATEGÍAS DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 22/12/2022	Código: DS-E-GET-23

También se establecen ejercicios funcionales permiten al personal validar su capacidad operativa para emergencias mediante la realización de sus funciones en un entorno operativo de contingencia. Los ejercicios funcionales están diseñados para ejecutar las funciones y responsabilidades de los miembros específicos del equipo, los procedimientos y los activos involucrados en uno o más funciones y aspectos del plan (por ejemplo, comunicaciones, notificaciones de emergencia), estos varían en complejidad y alcance, la validación de los aspectos específicos de un plan de ejercicios a escala real que se ocupan de todos los elementos del plan. Ejercicios funcionales permiten al personal evaluar sus funciones y responsabilidades como lo harían en una situación real de emergencia, pero en forma simulada.

4. Alcance de la Metodología de pruebas

El uso y desarrollo de esta metodología se define para las estrategias definidas en la mitigación de los escenarios de riesgo de interrupción de las funciones del Ministerio y especialmente ante la definición del Plan de Recuperación ante desastres DRP.

4.1. Tipos de prueba

Se definen tres tipos de prueba; de escritorio, por componentes y prueba integral como parte de un ejercicio progresivo, que se describen a continuación:

4.1.1. Prueba de Escritorio.

Se realiza un ejercicio en papel, de un escenario que toma lugar en un salón de conferencia real o virtual, en donde se establecen de acuerdo con el alcance y objetivos definidos; los participantes o involucrados, la lista de chequeo de los aspectos a verificar, la creación del escenario de desastre y la discusión alrededor de este, identificando todos los aspectos, actividades y recursos requeridos para mitigar el riesgo ocasionado por la materialización de este escenario.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	METODOLOGÍA DE PRUEBAS PARA ESTRATEGÍAS DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 22/12/2022	Código: DS-E-GET-23

4.1.2. Prueba por componentes.

Se ejecutan las estrategias y procedimientos (Tecnológicos y operativos) de recuperación de cada uno de los componentes de los diferentes servicios de TI y las aplicaciones que soportan los procesos considerados como críticos.

4.1.3 Prueba Integrada.

En donde se prueban los componentes en conjunto que hacen parte de la arquitectura de recuperación del DRP con base en el escenario definido, desarrollando las diferentes actividades y procedimientos del DRP, contando además con el apoyo de los funcionarios y proveedores que hacen parte del plan

5. Tipos de Alcance

- a) **Simulación.** Este alcance se define para probar en ambientes simulados o con datos de prueba.
- b) **Prueba en ambiente real.** Este alcance recrea un evento en condiciones controladas para evaluar un escenario de desastre en todos sus aspectos.

6. Procedimiento de recopilación de pruebas

Los procedimientos de recopilación de pruebas definidos son:

- Lista de chequeo (*checklist*): No es una prueba formal, pero sirve para empezar el plan y consiste en distribuir copias del plan de la prueba a todos los involucrados de la organización, estos deben revisarlo y aceptarlo.
- Discusión en mesa redonda (*tabletop*): permite descubrir dependencias o relaciones entre los distintos departamentos. Se reúne a todos los involucrados y se sigue el plan, línea por línea, construyendo un minuto grama.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	METODOLOGÍA DE PRUEBAS PARA ESTRATEGÍAS DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 22/12/2022	Código: DS-E-GET-23

- Ensayo (*walkthrough*): permite comprobar que todos los involucrados en el plan pueden seguir y cumplir con su deber. Consiste en llevar a cabo una simulación en terreno de la contingencia siguiendo paso a paso el plan.
- Funcional: permite aplicar el plan de contingencia, moviendo los servicios a un sitio alternativo.
- Interrupción total: consiste en interrumpir intencionalmente el servicio productivo y aplicar el plan de recuperación. Es la alternativa de prueba de mayor costo y tiempo, que recrea la realidad del desarrollo del DRP.

El siguiente cuadro esquematiza el flujo del desarrollo de la metodología de pruebas planteado en donde se desarrollan las pruebas por etapas cubriendo los tipos de pruebas con los diferentes métodos de recopilación en los diferentes ambientes de simulación y real.

	Checklist	Tabletop	Walkthrough	Funcional	Interrupción total
Prueba de Escritorio	👍	👍	👍	👍👍	👍
Prueba por componentes	👍	👍	👍👍	👍👍	👍
Prueba Integrada	👍	👍	👍	👍👍	👍👍

Cuadro flujo de la metodología de pruebas